IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

IN THE MATTER OF THE SEARCH OF 168 MONTLEY HILL LANE, HILLSVILLE, VIRGINIA, AND THE PERSON OF MICHAEL TIBBS	Case No. 7-24-mj-95 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Ryan Kennedy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search 168 Montley Hill Lane, Hillsville, Virginia, 24343, (the "PREMISES") believed to be the residence of MICHAEL TIBBS ("TIBBS").

2. I am a Special Agent with the FBI and have been so employed since August 2021. I currently work in the FBI Richmond, Virginia, Field Office, Roanoke Resident Agency. I am assigned to work a variety of criminal and national security matters, including the investigation of violent crimes, narcotics offenses, and major offenses such as federal bank robberies and the apprehension of federal fugitives. I have received training and gained experience in conducting investigations, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, and various other criminal laws and procedures.

PURPOSE OF AFFIDAVIT

3. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1470 (Transfer of Obscene Material to Minors), 2251 (Sexual Exploitation of Children and Attempted Sexual Exploitation of Children), 2252A (Certain

Activities Relating to Material Constituting or Containing Child Pornography), and 2422(b) (Coercion and Enticement) have been committed by TIBBS. There is also probable cause to search the location described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

4. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of and for the items described in Attachments A and B for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this Affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

STATUTORY AUTHORITY

5. 18 U.S.C. § 1470 prohibits the use of the mail or any facility or means of interstate or foreign commerce from knowingly transferring obscene matter to another individual who has not attained the age of sixteen years, knowing that such other individual has not attained the age of sixteen years.

6. 18 U.S.C. § 2251(a) prohibits, among other things, a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in any sexually explicit conduct for

the purpose of producing any visual depiction of such conduct, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2251(e) also prohibits attempts to violate § 2251(a).

7. 18 U.S.C. § 2252A(a) prohibits, among other things, a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate commerce, or affecting interstate commerce. 18 U.S.C. § 2252A(b) also prohibits attempts to violate the first six paragraphs of § 2252A(a).

8. 18 U.S.C. § 2422(b) prohibits, among other things, a person from knowingly persuading, inducing, enticing, or coercing a minor to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or to attempt to do so.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

10. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

11. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

12. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

13. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

14. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc, or other electronic means that is capable of conversion into a visual image, and data that is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

15. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

16. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252, 2256(2).

17. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

18. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

19. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

20. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a

range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

21. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

22. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

23. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

24. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

25. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up

Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

26. "Discord" is a free communications app that allows its users to share voice, video, and text chat with persons on the Internet as well as browse and share any website content with those whom the user selects while still within the Discord platform. Unlike other messaging apps, Discord usernames - not phone numbers - are the basis for Discord user accounts. Discord usernames are unique, can never be replicated, and are the only publicly available identifier Discord can use to identify a Discord account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address. Each unique username has a corresponding unique User ID.

BACKGROUND RELATING TO DISCORD

27. Discord owns and operates a free, all-in-one voice and text chat application and website of the same name that can be accessed at http://www.discordapp.com. Discord allows its users to establish accounts with Discord, which can then use to communicate with other Discord users. When signing up for a Discord account, the user must agree to Discord's Terms of Service.[1] Since at least March 28, 2022, Discord's Terms of Service have required users to abide by Discord's "Community Guidelines," which were also incorporated into the Terms of Service. The Community Guidelines that were in effect until March 27, 2023[2], told users: "Do not organize,

[1] Discord last updated its Terms of Service on March 15, 2024, effective April 15, 2024. The current Terms of Service may be accessed online at https://discord.com/terms. The Terms of Service that were in effect from March 28, 2022, until March 27, 2023, may be accessed online at https://discord.com/terms/terms-of-service-march-2022.

[2] Discord updated its Community Guidelines on March 15, 2024, effective April 15, 2024. The current Community Guidelines may be accessed online at https://discord.com/guidelines. The Community Guidelines that were in effect from March 28, 2022, until March 27, 2023, may be accessed online at https://discord.com/terms/guidelines-march-2022.

promote, or engage in any illegal or dangerous behavior, such as sexual solicitation . . . . These activities are likely to get you kicked off Discord, and may get you reported to law enforcement." They also warned users: "Do not sexualize children in any way. You cannot share content or links which depict children in a pornographic, sexually suggestive, or violent manner . . . ." Discord's current Community Guidelines are even more specific about its prohibitions on sexualizing children, soliciting sexual content from minors, and grooming minors.

28. Discord asks users to provide basic contact information to Discord, either during the registration process or thereafter. The information may include the user's full name, birth date, contact email addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Discord also assigns a user identification number to each account.

29. Discord users can exchange private messages on Discord with other users as well as participate in chat room discussions and voice chat.

PROBABLE CAUSE

30. On April 6, 2023, a minor female ("Minor A"), who lives in Georgia, submitted an online tip to the FBI National Threat Operations Center. The tip claimed that Minor A had been groomed online for approximately one year by a man who continually requested nude images despite having knowledge of her young age.

31. Minor A met Discord user Michael2242#3962, hereinafter referred to as "MICHAEL," in November 2022. MICHAEL told Minor A that he was 20 years old and from Virginia. Minor A informed MICHAEL that she was 14 years old. Minor A agreed, in exchange for money, to play video games with MICHAEL and to send him daily outfit pictures and good morning and good night texts. MICHAEL sent payments to Minor A via her CashApp account.

32. Minor A's conversations with MICHAEL eventually turned sexual. While on voice calls, MICHAEL told Minor A that he wanted to "eat her out" and "force her to give him oral." MICHAEL asked Minor A to send him nude pictures of her thighs, underwear, breasts, and vagina. Minor A told MICHAEL she would send him the images in exchange for money. Minor A set a price for the pictures, and after MICHAEL sent her the money, Minor A sent him the requested pictures via Discord, except that Minor A did not send MICHAEL any images of her vagina. MICHAEL sent Minor A an image of his penis via Discord.

33. On April 25, 2023, an FBI agent collected Minor A's cell phone. A review of the cell phone revealed a screenshot of Discord communications between Minor A and a Discord user with the username Michael2242#3962. The communications identified Minor A as a minor, showed child erotica sent from Minor A to MICHAEL, and showed an image of an exposed penis that MICHAEL sent to Minor A.

34. On April 28, 2023, a Child and Adolescent Forensic Interview was completed with Minor A. Minor A described a Discord server called "Discord Kittens" where people can sell experiences to other individuals in exchange for money. Minor A likened the experiences to being "someone's girlfriend." Inside of the servers, participants are separated into different channels for buyers and sellers. Sellers would sell services such as playing video games together, sending good morning and good night messages, and matching profile pictures. Sellers would sell their menu of services to buyers for them to pick. Minor A stated that on the Discord server people could sell anything other than items that were "not safe for work," meaning anything sexual in nature. During the interview, Minor A identified MICHAEL's CashApp as $miketibbs2243. Minor A also identified images of child erotica of herself that were sent to MICHAEL at his behest, and identified an image of an exposed penis as an image that MICHAEL had sent to her.

35. On May 23, 2023, an administrative subpoena was served on Discord, Inc., for the subscriber information for Michael2242#3962. The subpoena results revealed that the User ID associated with that account is 954239253485875212, and the associated email address and phone number are tibbs170@gmail.com and 276-733-1201 (the "1201 number"), respectively. The subpoena results also revealed that between November 17, 2022, and May 22, 2023, there were approximately 8,427 IP address log ins. Of those, the IP address 73.120.34.182 was used approximately 5,458 times. That IP address resolved to Comcast Cable.

36. On May 23, 2023, an administrative subpoena was served on Comcast Cable for the subscriber information related to the IP address 73.120.34.182. The subpoena results provided a subscriber name of a woman, who, according to open-source records, appears to be TIBBS's sister. The service and billing address was the same address as the PREMISES. The subscriber phone number was 276-733-4348 (the "4348 number"). Open-source records show that this is a cell phone that is registered in the name of a woman who appears to be TIBBS's mother.

37. On June 8, 2023, an administrative subpoena and a nondisclosure order was served on Google, Inc., for information related to the account tibbs170@gmail.com. The subpoena results provided, among other things, a subscriber name (Michael Tibbs), a Google Pay Address in Hillsville, Virginia (without a specified street address), and a Google Pay Contact (the 4348 number).

38. On May 22, 2023, an administrative subpoena was served on Block, Inc., for the account information pertaining to CashTag $miketibbs2243. The subpoena results provided that that account was associated with the following information: the name Michael Tibbs; date of birth February 22, 2001; the 1201 number as the telephone number; and the address was the same address is the PREMISES. Between October 20, 2019, and June 3, 2023, there were approximately

173 logins to that account. Of those, approximately 97 logins were from the IP address referenced above, 73.120.34.182. Between November 11, 2022, and April 7, 2023, there were approximately 16 payments sent from $miketibbs2243 to Minor A, totaling approximately $331.

39. Open-source and law enforcement database research for the 1201 number revealed that the telephone number belongs to Michael Tibbs, date of birth February 22, 2001, with a home address located at the PREMISES.

PREMISES

40. On May 21, 2024, the FBI conducted surveillance of TIBBS at his workplace at 1877 Carrollton Pike, Hillsville, Virginia. His workplace is 3.6 miles from his residence at the PREMISES. At approximately 8:00 PM, a white Subaru Outback, driven by an unknown female, arrived at the workplace. TIBBS climbed into the passenger seat, and they drove back to the residence. The Outback had previously been observed parked at the residence on multiple occasions. The vehicle is registered to the residence under the name of the subscriber of the 4348 number, who appears to be TIBBS's mother.

VIOLATION BACKGROUND

41. Computer/smartphone technology has revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography was historically produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone

calls. The development of computers/smartphones has changed this. Computers/smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

42. Child pornography offenders can now transfer photographs onto a computer readable format with a scanner. With the advent of digital cameras/smartphones, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

43. The computer/smartphone ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

44. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

45. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. These online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can still be found on the user's computer in most cases.

46. Digital files such as movies and pictures can be quickly and easily transferred back and forth between computers, smartphones, and other devices or stored simultaneously on multiple devices. Collectors of child pornography often keep their child pornography in multiple places, including on multiple devices.

47. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (e.g., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally (e.g., traces of the path of an electronic communication may be automatically stored in many places, such as in temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, was using Yahoo! Messenger, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

ADDITIONAL INFORMATION AND/OR CHARACTERISTICS

48. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who solicit and distribute child pornography.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain any hard copies of child pornographic material (i.e., pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc.) in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals, including those that create and/or produce child pornographic images, often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individual's computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if someone uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in their home.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

49. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

50. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

51. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes identified, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or

cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that, when an individual uses a computer to obtain child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

52. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires

considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the

entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

54. I know that a majority of households in the United States have access to a personal computing device of one type or another. In light of this fact, I believe that records associated with illegal conduct are likely to be found on digital devices, including "smartphones." Thus, I have requested permission to search digital devices that are found at the PREMISES.

55. Information stored in electronic form on all of the digital devices can provide evidence of crimes and identity of associates. For example, numbers stored in the telephones (such as Caller ID lists reflecting recently received calls, speed dial lists of names and/or telephone/contact numbers, and logs of outgoing and incoming calls) can provide evidence of who the subject is calling, and thus the identity of potential associates. Cellular telephones and other communication devices can contain similar information.

56. It is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from January 31, 2024, the Pew Research Center for Internet & Technology estimated that 97% of Americans owned at least one cellular phone, and that 90% of Americans owned at least one smartphone. *See* Mobile Fact Sheet, https://www.pewresearch.org/internet/fact-sheet/mobile/ (last visited July 1, 2024).

57. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smartphones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended

for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

58. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following: Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500-gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

59. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment and also can require substantial time. Further, evidence of how a digital device has been used, what it has been used for, and who has used it may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows

someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment and can require substantial time. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

60. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc., ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the

device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

61. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes, and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

62. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

63. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

64. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive or has not been unlocked for a certain

period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

65. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

66. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect

to TIBBS only: (1) compel the use of his thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of his face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

67. Further, there is probable cause to believe that evidence, fruits and instrumentalities of this crime are currently stored on the items which are described in Attachment A of this affidavit. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

68. The government would, if the cell phone is accessible/unlocked, seek to disable the mobile devices cellular data/Wi-Fi capabilities (i.e., airplane mode) before compelling the subject to utilize his biometric fingerprint to unlock any application within the device. The government may not be able to obtain the contents of the devices unless such biometric features are used to access the devices. Although I do not know which biometric features may be used to access any given device, I know based on my training and experience that it is common for people to use one of those features, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

69. The proposed warrant does not authorize law enforcement to require that TIBBS state or otherwise provide the password or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access any digital

devices within the scope of the requested warrant. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel TIBBS to state or otherwise provide that information. However, the voluntary disclosure of such information by TIBBS would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask TIBBS for the password to any digital devices within the scope of the requested warrant, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any digital devices within the scope of the requested warrant, the agents will not state or otherwise imply that the warrant requires the person to provide such information and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

70. Law enforcement personnel will commence the execution of this search and seizure warrant upon the PREMISES during daytime hours (between 6:00 a.m. and 10:00 p.m.), as early as practicable. It is anticipated that law enforcement personnel may attempt to image or copy digital information from storage media located on the PREMISES rather than remove that storage media from the premises. Such onsite imaging or copying will minimize disruptions to the use of that storage media.

71. From my training and experience, I know that imaging or copying information from storage media on PREMISES can be substantially delayed by various factors that cannot be ascertained or sometimes even anticipated until the actual execution of the warrant. There may, for example, be no system administrator available, willing, or able to assist law enforcement personnel to narrow the search by identifying the virtual or dedicated storage media on the PREMISES, or the folders containing information within the scope of the warrant. There may be terabytes or even petabytes of information to be copied. The network architecture of the storage

media on the PREMISES or the configuration of the hardware may affect and delay data transfer speeds. Data encryption and password protections may also significantly delay imaging or copying as law enforcement personnel seek to identify necessary passwords without which imaging or copying on the PREMISES would likely be unachievable. Under some circumstances, data downloads can be interrupted by network or hardware malfunctions or other network or hardware attributes, which often necessitates restarting the data downloads from the beginning.

72. Law enforcement personnel will commence executing the warrant as near to 6:00 a.m. as practicable. However, given the myriad factors that that may prevent completion of the search and seizure by 10:00 p.m., including those described above, I request authorization to continue the warrant execution past 10:00 p.m., if necessary, until completion of the warrant execution. Suspending the execution at 10:00 p.m. until 6:00 a.m. the following day could compromise data downloads in progress, render stored data subject to alteration or deletion, require securing the PREMISES during the intervening hours, and prolong the disruption of access to, and use of, the PREMISES and the digital devices being searched.

ADDITIONAL REQUEST TO SEARCH THE PERSON OF TIBBS

73. It is common for investigative subjects and evidence of interest to be absent from the place to be searched but still in the local area when law enforcement executes a search warrant. It is possible that TIBBS will not be present at the PREMISES during the execution of the requested search warrant.

74. I am aware that individuals commonly keep electronic devices on their person when they leave their residence. This is especially true of devices that may contain contraband or are utilized for criminal activity. Moreover, in cases involving electronic evidence, it is critical to

locate and obtain that evidence before the subject becomes aware of law enforcement's intentions to seize and search to prevent such evidence from being hidden, destroyed, or otherwise altered.

75. Therefore, if agents positively locate and identify TIBBS within the Western District of Virginia outside the residence to be searched, or in a public place, or within a motor vehicle or other conveyance, I request the following authorization:

a. To briefly detain TIBBS to search his person; and

b. If TIBBS is encountered in a vehicle, to search portions of the vehicle that he has reasonable control over, or access to, for the items listed in Attachment B of this application. For example:

i. If TIBBS has the keys to and is operating a vehicle that he has clear use, dominion, and control over, then it would be reasonable for Agents to search for items within all areas of the vehicle including the passenger compartment, trunk, and personal containers found within.

ii. If TIBBS is encountered as a passenger in a vehicle that he is a guest in and does not have dominion and control over, then it would be reasonable for Agents to search for items within areas of the vehicle he has access to including the passenger compartment or his personal containers found within.

CONCLUSION

76. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant as there is probable cause to believe that the federal criminal statutes cited herein have been violated and that the evidence of these offenses, more fully described in Attachment B of this Application, are located at the PREMISES, described further in Attachment A. I respectfully

request that this Court issue a search warrant for the PREMISES, authorizing the seizure and search of the items described in Attachments B.

Respectfully submitted,

Ryan Kennedy

Ryan Kennedy
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me by telephone on July 15, 2024

Hon. C. Kailani Memmer
UNITED STATES MAGISTRATE JUDGE